

REMARKS

This amendment is filed in response to the Office action dated April 23, 2007. Claims 9-18 and 30-38 are canceled. By this amendment, claims 1, 7, 19, 20, 23 and 30 are amended to correct antecedent usage and provide clarification. Claims 19-23, 26 and 27 are amended in response to Examiner remarks. Claims 1-8 and 19-30 are now pending and at issue in this application. Applicants respectfully request reconsideration of the claims and favorable action in this case.

Response to Rejections of Claims at Issue**Claim Objections:**

Claim 19 has been amended to correct antecedent usage as specified by the Examiner.

Claim Rejections under 35 U.S.C. § 101:

Claims 19-22 were rejected under 35 U.S.C § 101 as being directed to data structures and not capable of causing functional change in the computer. The Applicants have amended Claims 19-22 to disclose a method of generating a data structure for implementing a name resolution protocol. Amended Claims 19-22 are in a condition for allowance.

Claims 23-30 were rejected under 35 U.S.C § 101 as being directed to non-statutory subject matter, specifically that the claims are directed to a signal without a physical structure that does not perform a useful, concrete and tangible result. The Applicants have amended claims 23-30 to claim “a computer-readable medium tangibly embodying a program of instruction executable by a computer for performing steps to...”. Accordingly, the Applicants believe that the amendments sufficiently limit the claims to exclude a non-tangible signal medium.

Claim Rejections under 35 U.S.C. §102(e):**Claims 1 and 23:**

Claims 1 and 23 were rejected as being anticipated by Yeager, et. al. (U.S. Patent Application Publication 2003/0070070 A1), hereinafter referred to as “Yeager”. Claims 1 and 23 disclose a method and a structure to provide name resolution that combines PNRP lookup techniques with DNS hierarchical lookups and SPKI type certifications. Rather than having a name and an authority resolve to an address as in PNRP and DNS, however, the name resolution technique can resolve to either an authority, an address, or a set of address, port name and protocol. Namespaces can include names with delegated authorities by creating an authority that is referred to without the administrative burden of DNS because the actual addresses of the delegated authorities are not required to be known to perform a lookup. The name resolution protocol thus may use more than one level of indirection to resolve names.

Yeager [0017] [0019] and [0164] do not disclose an embodiment of generating one or more cryptographic keys associated with a namespace for the purposes of creating an authority. Yeager [0017] and [0019] teach generating keys and certificates to support a trust mechanism or spectrum for certificate distribution as defined in Yeager [0003]. Yeager [0164] also does not disclose an embodiment of generating one or more cryptographic keys associated with a namespace for the purposes of creating an authority. Yeager [0164] discusses publishing a source for lists of addresses for peer authorization services.

Yeager [0162] does not disclose creating an authority using one of the cryptographic keys for use in enabling lookups between connected devices. The first sentence of Yeager [0162] bounds the embodiment of creating a peer identity to be used in a PGP (“Pretty Good Privacy”) certificate for use in a trust spectrum. Claims 1 and 23, on the other hand, are directed to creating an authority (identity) for use in enabling lookups between connected devices, as stated in the preambles of Claims 1 and 23.

Yeager [0152] discusses an overall architecture of peer groups, peer identities, and uniqueness of certificates issued to peers. It does not disclose enabling a namespace (identity) to resolve to the authority created in the earlier steps of Claims 1 and 23.

Yeager [203] discusses an embodiment of using a UUID as part of a peer name in a peer-to-peer platform. It does not disclose how the name is used in a name resolution protocol using multiple levels of indirection for resolution.

The cited paragraphs from Yeager discussed above do not disclose all the elements taught by Claims 1 and 23. Therefore, Claims 1 and 23 are not anticipated by Yeager and are under condition for allowance.

Claims 2 and 24

Both Yeager and this application describe embodiments in a peer-to-peer network cloud. However, Yeager discloses “a trust spectrum for certificate distribution in distributed peer-to-peer networks” [0003] whereas this application teaches a name resolution technique that can resolve to either an authority, an address, or a set of address, port name and protocol. Furthermore, since Claims 1 and 23 are in condition for allowance as discussed above, and dependent Claims 2 and 24 further limit Claims 1 and 23 respectively, Claims 2 and 24 are not anticipated by Yeager and are also under condition for allowance.

Claims 3 and 25

As discussed above for Claims 1 and 23, Yeager [0152] describes an overall architecture of peer groups, peer identities, and uniqueness of certificates issued to peers. Yeager [0164] discusses publishing a source for lists of addresses for peer authorization services. Neither cited paragraph discloses enabling a namespace (identity) to resolve to the authority created as per Claims 1 and 23 by using namespaces and their names as inputs. Claims 3 and 25 are not anticipated by Yeager [0152] and [0164] and therefore are under condition for allowance.

Claims 4 and 26

Yeager [0233] provides a general description of peer services. Yeager [0234] defines peer endpoints in peer network interfaces, and using intermediary peers for routing between endpoints. Neither paragraph discloses an approach using multiple levels of indirection to enable a namespace (identity) to resolve to the authority created as per Claims 1 and 23, and

publishing the created authority and a service name to receive data. Claims 4 and 26 are not anticipated by Yeager [0233] and [0234] and therefore are under condition for allowance.

Claims 5 and 27

Yeager [0199] provides another general description that discusses how protocol bindings are used to create a peer-to-peer platform. It does not disclose an approach using multiple levels of indirection to enable a namespace (identity) to resolve to the authority created as per Claims 1 and 23, and publishing the created authority and a service name to receive an IP address, a protocol name and a port identity. Claims 5 and 27 are not anticipated by Yeager [0199] and therefore are under condition for allowance.

Claims 6 and 28

As discussed above, Yeager [0203] discusses an embodiment of using a UUID as part of a peer name in a peer-to-peer platform. Yeager [0311] gives a generalization of dynamic routing in a peer-to-peer network by using discovery messages to/from intermediate rendezvous peers to reconfigure routing. Both paragraphs do not disclose dynamically changing an address associated with the authority created as per Claims 1 and 23 to another name associated with one or more addresses for use in a name resolution method using multiple levels of indirection. Claims 6 and 28 are not anticipated by Yeager [0203] [0311] and therefore are under condition for allowance.

Claims 7 and 29

Yeager [0372] defines a codat and gives examples of them. Lines 8 and 9 state: “Codats are the elementary unit of information that is exchanged between peers.” Claims 7 and 29, however, disclose an approach using multiple levels of indirection to enable a namespace (identity) to resolve to the authority created as per Claims 1 and 23, and further resolving to one of the group arbitrary data, hosts and services. Claims 7 and 29 are not anticipated by Yeager [0372] and therefore are under condition for allowance.

Claims 8 and 30

As previously discussed above, Yeager [0162] teaches the embodiment of creating a peer identity to be used in a PGP (“Pretty Good Privacy”) certificate. Yeager [0162] does not

disclose creating an authority using a hash of a cryptographic key for use in enabling lookups between connected devices. Claims 8 and 30 are not anticipated by Yeager [0162] and therefore are under condition for allowance.

Claim 19

Yeager [0017] and [0162] do not disclose an embodiment of generating one or more cryptographic keys associated with a namespace for the purposes of creating an authority. As discussed above, Yeager [0017] discusses generating keys and certificates to support a trust mechanism or spectrum for certificate distribution as defined by Yeager [0003]. Yeager [0162] teaches the embodiment of concatenating name identifiers for use in a PGP certificate. Yeager [0164] discusses publishing a source for lists of addresses for peer authorization services. Yeager's claims also support the description by teaching towards the uses of keys and certificates for a use in a trust spectrum and not for a method of generating a data structure to support implementation of a name resolution protocol. Therefore, Claim 19 is not anticipated by Yeager [0017] [0162] [0164].

Claim 20

As previously discussed, Yeager [0199] generally describes how protocol bindings are used to create a peer-to-peer platform. It does not disclose a method of generating a data structure to support implementation of a name resolution protocol where the authority of the first field and the name of the second field can be resolved to an IP address, a protocol name and a port identity. Claim 20 is not anticipated by Yeager [0199] and therefore is under condition for allowance.

Claim 21

Yeager [0372] defines a codat and gives examples of codats. Yeager [0372] does not disclose a method of generating a data structure to support implementation of a name resolution protocol where the authority of the first field and the name of the second field can be resolved to arbitrary data. Claim 21 is not anticipated by Yeager [0372] and therefore is under condition for allowance.

Claim 22

Yeager [0219] provides a general discussion of how information may be cached on various peers in the network for other peers to find. Yeager [0233] defines peer services at a high level and how they may also be cached. Yeager [0315] describes caching advertisements and discovery information. Yeager [0219] [0233] and [0315] do not disclose a method of retrieving an IP address, protocol name, and/or port number from a cache for use in a data structure supporting the implementation of a name resolution protocol. Claim 22 is not anticipated by Yeager [0219] [0233] and [0315] and therefore is under condition for allowance.

CONCLUSION

In view of the above amendments and arguments, the Applicants submit that claims 1-8 and 19-30 of the pending application are in condition for allowance and an early action so indicating is respectfully requested.

If the Examiner has any questions, the Examiner is encouraged to call the undersigned at (312) 474-6300. Applicants believe no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 13-2855, under Order No. **30835/303114** from which the undersigned is authorized to draw.

Dated: August 1, 2007

Respectfully submitted,

By /Jeffrey K. Berger/

Jeffrey K. Berger

Registration No.: 51,460

MARSHALL, GERSTEIN & BORUN LLP

233 S. Wacker Drive, Suite 6300

Sears Tower

Chicago, Illinois 60606-6357

(312) 474-6300

Agent for Applicants